BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

#3

(Translation)

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application : July 3, 2000

Application Number : Patent Appln. No. 2000-201650

Applicant(s) : SHARP KABUSHIKI KAISHA

Wafer of the Patent Office

May 30 2001

Kozo OIKAWA

Commissioner,
Patent Office

Seal of Commissioner of the Patent Office

Appln. Cert. No. Appln. Cert. Pat. 2001-3047867

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　７月　３日

出願番号
Application Number: 特願２０００－２０１６５０

出願人
Applicant(s): シャープ株式会社

２００１年　５月３０日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０４７８６７

【書類名】　特許願
【整理番号】　00J02070
【提出日】　平成12年 7月 3日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 12/14
【発明者】
　【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内
　【氏名】　友広　一郎
【特許出願人】
　【識別番号】　000005049
　【氏名又は名称】　シャープ株式会社
【代理人】
　【識別番号】　100078282
　【弁理士】
　【氏名又は名称】　山本　秀策
【手数料の表示】
　【予納台帳番号】　001878
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9005652
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　半導体記憶装置

【特許請求の範囲】

【請求項１】　電気的に一括消去可能な単数または複数の不揮発性のメモリセルアレイブロックを有し、システムに組み込まれたときにシステムからのデータの書き換えを制限するセキュリティ機能を有する半導体記憶装置であって、

該メモリセルアレイブロック内に設けられ、セキュリティ解除鍵が格納されるメモリ領域と、

保護されるメモリセルアレイブロック毎に対応するセキュリティ登録錠が格納される不揮発性記憶手段と、

該セキュリティ解除鍵と該セキュリティ登録錠の値そのもの、または該セキュリティ解除鍵および該セキュリティ登録錠の各々を用いて生成される値を比較照合して、セキュリティ解除の許可を行うか否かを判定する判定回路と、

該判定回路からの出力信号が、該セキュリティ解除鍵と該セキュリティ登録錠の比較照合結果が一致したことを示している場合に、該当するメモリセルアレイブロックからの読み出しデータが外部に出力されるのを許可する正規データ出力許可回路と

を備えた半導体記憶装置。

【請求項２】　前記セキュリティ解除鍵と前記セキュリティ登録錠の比較照合結果を保存するレジスタを備え、該レジスタの出力信号が、該セキュリティ解除鍵と該セキュリティ登録錠の比較照合結果が一致したことを示している場合に、前記正規データ出力許可回路が該当するメモリセルアレイブロックからの読み出しデータが外部に出力されるのを許可する請求項１に記載の半導体記憶装置。

【請求項３】　前記セキュリティ解除鍵および前記セキュリティ登録錠の少なくとも一方を、対応する格納部に書き込むために外部から入力される設定命令を解釈する命令解釈手段を有する請求項１または請求項２に記載の半導体記憶装置。

【請求項４】　全てのメモリセルアレイブロックまたは一部のメモリセルアレイブロックに対して、前記セキュリティ解除鍵と前記セキュリティ登録錠の比

較照合を行い、その結果を一括して前記レジスタに書き込む請求項２に記載の半導体記憶装置。

【請求項５】　一方向変換回路または暗号回路を有し、該一方向変換回路または該暗号回路によって前記セキュリティ解除鍵および前記セキュリティ登録錠を変換した結果を、前記メモリ領域および前記不揮発性記憶手段に書き込む請求項１乃至請求項４のいずれかに記載の半導体記憶装置。

【請求項６】　前記セキュリティ解除鍵および前記セキュリティ登録錠を読み出す手段が備わっていない請求項１乃至請求項５のいずれかに記載の半導体記憶装置。

【請求項７】　前記不揮発性記憶手段が書き換えおよび消去を禁止するワンタイムプログラマブルロムであり、セキュリティ登録錠の書き込み後に書き換えおよび消去を禁止するか、または不揮発性のロック機能を有し、セキュリティ登録錠の書き込み後にロックをかけてセキュリティ登録錠の書き込み後に書き換えおよび消去を禁止する請求項１乃至請求項６のいずれかに記載の半導体記憶装置。

【請求項８】　前記セキュリティ解除鍵の設定フラグを有し、該セキュリティ解除鍵の書き込み後に該設定フラグを自動または手動で設定することにより、該当するメモリセルアレイブロックへの追加書き込みを禁止する請求項１乃至請求項７のいずれかに記載の半導体記憶装置。

【請求項９】　前記セキュリティ解除鍵を前記メモリ領域に書き込み中に、ウェイト動作を行う請求項１乃至請求項８のいずれかに記載の半導体記憶装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、半導体集積回路等に用いられる不揮発性のメモリセルアレイブロックを有する半導体記憶装置に関し、特に、メモリに格納されている内容が不正に改ざんされることを防ぐためのセキュリティ機能を備えた半導体記憶装置に関する。

【０００２】

【従来の技術】

フラッシュメモリに代表される電気的に消去可能な不揮発性半導体記憶装置は、システム上でデータの書き換えが可能であり、システム組み立て後もデータやコードの更新を行うことが可能である。このため、マイクロコンピューター等を用いたシステムを所望の手順に従って動作させるためのプログラムを格納するために、このような不揮発性半導体記憶装置が広く用いられる。この場合、利用者認証のための情報や検査プログラム等も同一記憶装置内に格納されるため、内容更新を容易に行うことができる手段が要求される一方で、不正なデータ書き換え（改ざん）を防止するための機能も要求される。

【０００３】

例えば特開平９－３２７９７号公報に開示されているように、従来実用化または提案されている改ざん防止回路においては、正規ユーザによる操作であるか否かを認証するために、機能限定解除キーコードを外部から入力するという方法で対処している。

【０００４】

図３は、従来のデータ改ざん防止回路が内蔵された半導体メモリを示す。この従来回路（ロック回路）は、一方向ハッシュ変換されたキーコードを保持する内部レジスタ３０と、入力された暗号に対する復号回路（保全通信回路）３１と、一方向ハッシュ機能を有する変換回路３２と、機能制限解除判定回路（比較回路）３３と、書き込み制御回路と、ゲート回路とを備えている。

【０００５】

このロック回路は、内部レジスタ３０に予め格納されている照合値（キーコード）を直接読み出された場合にデータを保護するため、照合値を平文で格納するのではなく、一方向ハッシュ変換回路３２によって変換した値を格納している。また、外部から入力される機能限定解除キーコードを保護するため、外部から入力される機能限定解除キーを暗号化している。その機能限定解除キーを保全通信回路３１で復号化した後（キーコードＩｖ１）、１方向ハッシュ変換回路３２により変換して（キーコードＩｖ２）、変換値により内部レジスタ３０に格納されている照合値とを比較回路３３で比較する。そして、一致照合した場合に機能制

限解除信号３４により機能限定を解除する。また、照合が成功するまで全パターンにわたってキー入力を試す繰り返し攻撃に耐えるために、保全通信回路３１をＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ　Ｋｅｙ　Ｅｘｃｈａｎｇｅアルゴリズム等により構成し、有効なキーが毎回変更されるようにしている。

【０００６】

【発明が解決しようとする課題】

しかしながら、上述した従来技術には、以下のような問題があった。

【０００７】

まず、機能限定を解除するためにデバイス外部から機能限定解除キーを入力する必要がある。このため、上記システムは、デバイス外部に機能限定解除キーを記憶しておくためのキー記憶装置を有する。しかし、デバイス間（ここでは図３のデバイスとシステム内の他のデバイス（キー記憶装置）の通信が暗号化されているとは言え、デバイス外に機能限定解除キーを有することになるため、アクセス許可を求める度にキーがインターフェイス部分を流れることになる。よって、機能限定解除キーが傍受されたり、または外部のキー記憶装置自体から直接読み出される危険性がある。

【０００８】

また、デバイス間の通信を暗号化するために、複雑な回路が必要である。特に、繰り返し攻撃に耐えるためには、複雑な暗号が必要であり、デバイス内部の復号化回路も複雑になる。

【０００９】

さらに、改ざん防止機能を有効にするためには、システム側が対応する必要があり、改ざん防止機能を有するデバイスに置き換えるだけでは利用できない。

【００１０】

本発明はこのような従来技術の課題を解決するためになされたものであり、メモリセルアレイブロックに格納されているデータを不正な改ざんから保護することができ、正規の書き換えが可能で、セキュリティ解除鍵が解読されにくく、不揮発性半導体記憶装置外部のシステムにセキュリティ解除鍵を保持しておく必要がなく、従来の不揮発性半導体記憶装置との互換性があり、不正ユーザによる認

証に対する繰り返し攻撃に強い半導体記憶装置を提供することを目的とする。

【００１１】

【課題を解決するための手段】

本発明の不揮発性半導体記憶装置は、電気的に一括消去可能な単数または複数の不揮発性のメモリセルアレイブロックを有し、システムに組み込まれたときにシステムからのデータの書き換えを制限するセキュリティ機能を有する半導体記憶装置であって、該メモリセルアレイブロック内に設けられ、セキュリティ解除鍵が格納されるメモリ領域と、保護されるメモリセルアレイブロック毎に対応するセキュリティ登録錠が格納される不揮発性記憶手段と、該セキュリティ解除鍵と該セキュリティ登録錠の値そのもの、または該セキュリティ解除鍵および該セキュリティ登録錠の各々を用いて生成される値を比較照合して、セキュリティ解除の許可を行うか否かを判定する判定回路と、該判定回路からの出力信号が、該セキュリティ解除鍵と該セキュリティ登録錠の比較照合結果が一致したことを示している場合に、該当するメモリセルアレイブロックからの読み出しデータが外部に出力されるのを許可する正規データ出力許可回路とを備えており、そのことにより上記目的が達成される。

【００１２】

前記セキュリティ解除鍵と前記セキュリティ登録錠の比較照合結果を保存するレジスタを備え、該レジスタの出力信号が、該セキュリティ解除鍵と該セキュリティ登録錠の比較照合結果が一致したことを示している場合に、前記正規データ出力許可回路が該当するメモリセルアレイブロックからの読み出しデータが外部に出力されるのを許可してもよい。

【００１３】

前記セキュリティ解除鍵および前記セキュリティ登録錠の少なくとも一方を対応する格納部に書き込むために外部から入力される設定命令を解釈する命令解釈手段を有していてもよい。

【００１４】

全てのメモリセルアレイブロックまたは一部のメモリセルアレイブロックに対して、前記セキュリティ解除鍵と前記セキュリティ登録錠の比較照合を行い、そ

の結果を一括して前記レジスタに書き込んでもよい。

【００１５】

一方向変換回路または暗号回路を有し、該一方向変換回路または該暗号回路によって前記セキュリティ解除鍵および前記セキュリティ登録錠を変換した結果を、前記メモリ領域および前記不揮発性記憶手段に書き込んでもよい。

【００１６】

前記セキュリティ解除鍵および前記セキュリティ登録錠を読み出す手段が備わっていないのが好ましい。

【００１７】

前記不揮発性記憶手段が書き換えおよび消去を禁止するワンタイムプログラマブルロムであり、セキュリティ登録錠の設定後に書き換えおよび消去を禁止するか、または不揮発性のロック機能を有し、セキュリティ登録錠の書き込み後にロックをかけてセキュリティ登録錠の設定後の書き換えおよび消去を禁止してもよい。

【００１８】

前記セキュリティ解除鍵の設定フラグを有し、該セキュリティ解除鍵の書き込み後に該設定フラグを自動または手動で設定することにより、該当するメモリセルアレイブロックへの追加書き込みを禁止してもよい。

【００１９】

前記セキュリティ解除鍵を前記メモリ領域に書き込み中に、ウェイト動作を行ってもよい。

【００２０】

以下、本発明の作用について説明する。

【００２１】

請求項１に記載の本発明にあっては、データを書き換えようとする場合、メモリセルアレイブロックの消去時に、該当ブロックのメモリ領域に格納されたセキュリティ解除鍵も消去される。よって、消去後に新しいデータを書き込んだ後、システムからの読み出し制限を解除するために、該当ブロック毎に不揮発性レジスタ等の不揮発性記憶手段に格納されているセキュリティ登録錠に対応するよう

に、セキュリティ解除鍵を再びメモリ領域に書き込む必要がある。このとき、正しいセキュリティ解除鍵は正規ユーザにしか分からないため、不正ユーザがメモリ内容を書き換えると、そのシステムを使用することができなくなる。よって、不正なデータ改ざん（不正な書き換え）を防ぐことが可能である。

【００２２】

一般に、フラッシュメモリに代表される電気的に消去可能な不揮発性半導体記憶装置においては、品質が保証される書き込み／消去回数に制限がある。このため、不正ユーザによるセキュリティ解除鍵に対する繰り返し攻撃（トライアンドエラー攻撃）に対しては、不揮発性半導体記憶装置の劣化を招くという作用も有する。さらに、フラッシュメモリにおいては、ブロックの消去はデータの読み出しや書き込みに比べて時間がかかるため、セキュリティ解除鍵に対する繰り返し攻撃（トライアンドエラー攻撃）に時間がかかり過ぎて、現実的ではないという作用も有する。

【００２３】

認証の際には、判定回路によって、セキュリティ解除鍵とセキュリティ登録錠とを比較照合し、その結果が一致している場合にセキュリティ解除を行うので、外部とセキュリティ解除鍵をやり取りしない。よって、従来技術のようにセキュリティ解除鍵が傍受されることはなく、セキュリティ機能が解読されにくい。また、従来技術のようにデバイス間の通信を暗号化するための複雑な暗号化回路や複雑な復号化回路を必要とせず、装置を簡略化することができる。また、装置外部のシステムにセキュリティ解除鍵を保持しておく必要がないため、従来技術のように外部のキー記憶装置自体からセキュリティ解除鍵が直接読み出されることはなく、また、改ざん防止のためにシステム側が対応する必要もない。

【００２４】

書き換えを行わない限り、セキュリティ機能が無いデバイスと同様に利用でき、不正な書き換えが行われた場合にはシステムが使えなくなるというセキュリティ機能が働くため、ユーザ／システム共にセキュリティ機能（パスワード）の存在を意識する必要がなく、従来のシステムに対しても互換性を有する不揮発性半導体記憶装置を提供することが可能である。なお、セキュリティ解除鍵を設定す

るためにはユーザがセキュリティ鍵を入力する必要があるので、パスワード（セキュリティ解除鍵）が必要になる。

【００２５】

正しいセキュリティ解除鍵を知っている正規ユーザは、データ書き換え後に正しいセキュリティ解除鍵をメモリ領域に書き込むことができるので、正規の書き換えは可能である。

【００２６】

請求項２に記載の本発明にあっては、各ブロック毎の比較照合結果を揮発性レジスタに保持しておくことにより、一度照合すれば、レジスタが値を保持している間はレジスタ値によりアクセス制限が可能となる。よって、請求項１に記載の本発明に比べて、不揮発性半導体記憶装置のアクセス速度の低下を防いで、ユーザにセキュリティ機能の存在を意識させないようにすることが可能である。このとき、揮発性レジスタを用いる理由は、以下の通りである。セキュリティ登録錠とセキュリティ解除鍵の認証をアクセスの度に行うと、アクセス速度の低下を招くが、揮発性レジスタを用いることにより、起動時に一度認証を行えば、それ以降のアクセス時に認証が不要となり、アクセス速度は低下しない。これに対して、不揮発性レジスタを用いた場合には、一度認証を行うと、それ以降はセキュリティ登録錠とセキュリティ解除鍵から認証するのではなく、不揮発性レジスタに格納された値を参照するだけになる。よって、不揮発性レジスタを何らかの手段で直接不正に書き換えることができ、または一旦設定された値を消去されないように不正な手段で実現することができた場合、以降のセキュリティが機能しないことになり、セキュリティとして弱いものになる。なお、後述する実施形態に示すように、セキュリティが不要なブロックに対しては、不揮発性レジスタに比較照合結果が一致していることを示す値を保持しておいてもよい。

【００２７】

請求項３に記載の本発明にあっては、ユーザがセキュリティ解除鍵またはセキュリティ登録錠と共に設定命令を入力すると、命令解釈手段が設定命令を解釈し、その出力信号に従ってセキュリティ解除鍵またはセキュリティ登録錠が対応する格納部に書き込まれる。これによって、不揮発性半導体記憶装置の製造および

出荷後でも各不揮発性半導体記憶装置に対して任意のセキュリティ登録錠を設定することができるので、セキュリティ登録錠の値を知っている者の人数を減らしてセキュリティを高めることが可能である。また、セキュリティ登録錠の値を組み込みシステム毎に変えることによりセキュリティを高めることができ、さらに、セキュリティ登録錠の値が不正ユーザに洩れたとしても、セキュリティ登録錠の値から本発明の不揮発性半導体記憶装置を使用したシステムの製造時期や製造工場等、システムの素性を明らかにして、セキュリティ登録錠が不正ユーザの手に渡った経緯を明らかにするのに役立てることが可能である。

【００２８】

なお、セキュリティ解除鍵の設定命令とセキュリティ登録錠の設定命令のいずれか一方だけを解釈するための命令解釈手段を設けてもよい。セキュリティ解除鍵の設定命令を実装しない場合、通常のデータ入力コマンドシーケンスにセキュリティ解除鍵データも含める方法等が考えられる。例えば、

１）プログラムコマンド

２）プログラムデータ数（ｎ）

３）～３＋ｎ）プログラムデータ列

ｎ＋４）セキュリティ解除鍵データ

というようなｎ＋４サイクルのコマンド体系もあり得る。

【００２９】

しかし、この場合には、従来デバイスとの互換性が取れなくなること、セキュリティ機能の存在が知られ易いこと、１ワード／バイト単位等、ブロックの一部を書き換えるコマンドでは、その度にセキュリティ解除鍵データを入力することになるため不便であることなどの欠点がある。これに対して、セキュリティ解除鍵の設定命令を独立したコマンドとして実装することにより、従来デバイスとの互換性を保ちつつ、セキュリティ機能を有するデバイスを実現することができ、不正改ざん者を含むシステム使用者にセキュリティ機能の存在を明らかにする必要もなくなる。さらに、請求項９のようなセキュリティに対する攻撃を防止するための機能を比較的自由に付加することが可能となる。

【００３０】

請求項４に記載の本発明にあっては、全てのメモリセルブロックまたは一部のメモリセルブロックに対して、セキュリティ解除鍵とセキュリティ登録錠の比較照合を行った結果が一括してレジスタに書き込まれるので、不揮発性半導体記憶装置のアクセス速度の低下を防ぐことが可能である。この場合、ユーザからの認証命令によって認証を行うようにしてもよく、また、装置の起動時やリセットからの復帰時に自動的に認証が実行されるようにしてもよい。

【００３１】

請求項５に記載の本発明にあっては、セキュリティ解除鍵およびセキュリティ登録錠が平文のままではなく、暗号化した形で格納されるので、セキュリティ解除鍵やセキュリティ登録錠が何らかの手段で不正ユーザに直接読み出された場合でも、データを改ざんするのが困難である。特に、逆変換が困難な一方向関数（例えば一方向ハッシュ関数）による変換が好ましいが、簡単な暗号回路であってもよい。但し、セキュリティ解除鍵を変換した結果が、セキュリティ登録錠を変換した結果と等しくなるような回路構成にする必要がある。

【００３２】

請求項６に記載の本発明にあっては、セキュリティ解除鍵およびセキュリティ登録錠を装置外部から読み出す手段が備わっていないため、解除錠および登録錠はライトオンリーレジスタとして機能する。この場合、セキュリティ解除鍵やセキュリティ登録錠が不正ユーザに直接読み出されてデータが改ざんされるのを防ぐことが可能である。

【００３３】

請求項７に記載の本発明にあっては、セキュリティ登録錠をワンタイムプログラマブルロムに設定することにより、セキュリティ登録錠の設定後に書き換え動作を禁止することが可能である。または、書き換え可能な不揮発性記憶手段を用いて、不揮発性のロックフラグ等のロック機能を設け、セキュリティ登録錠の書き込み後にロックをかけてもよい。これにより、セキュリティ登録錠自体が不正に書き換えられるのを防ぐことが可能である。

【００３４】

請求項８に記載の本発明にあっては、セキュリティ解除鍵の設定フラグを設定

することにより、セキュリティ解除鍵の書き込み後に該当ブロックへの追加書き込みが禁止される。このとき、セキュリティ解除鍵が不正なものである場合には、該当ブロックへの読み出しに対しては全て消去値を出力する等の偽のデータが出力される。よって、不正ユーザがセキュリティ解除鍵への繰り返し攻撃を行う際には、セキュリティを解除できたかどうかを確認できるように、セキュリティ解除鍵の入力を試みる前に、該当ブロックへのデータ書き込みを行う必要がある。このため、一回当たりの挑戦に要する時間が長くなって、セキュリティ解除鍵を解析するのが困難になる。

【００３５】

請求項９に記載の本発明にあっては、セキュリティ解除鍵を設定中に、ウェイト動作を行うので、通常のメモリセルアレイブロックへの書き込み動作よりも著しく時間がかかる。よって、不正ユーザによるセキュリティ解除鍵への繰り返し攻撃の際に、一回当たりの挑戦に要する時間が長くなって、セキュリティ解除鍵を解析するのが困難になる。

【００３６】

【発明の実施の形態】

以下に、本発明の実施の形態について、図面を参照しながら説明する。

【００３７】

図１は、本発明の一実施形態である不揮発性半導体記憶装置の構成を説明するためのブロック図である。

【００３８】

この不揮発性半導体記憶装置は、フラッシュＥＥＰＲＯＭ回路であり、アドレスプリデコーダ１９、カラムデコーダ１７、ローデコーダ１８、ブロックデコーダ１０、電気的に一括消去可能な単数または複数の不揮発性メモリセルアレイブロック１１、各メモリセルアレイブロックｎに対応するセキュリティ登録錠が格納された不揮発性レジスタ１３、セキュリティ解除判定回路１４、各ブロックｎに対する判定結果保存レジスタ１５、メモリセルアレイデータ出力切り替え回路１６から構成されている。

【００３９】

メモリセルアレイブロック１１は、ユーザがデータ記憶のために使用することができるメインメモリブロック領域１１ａと、メインメモリのアドレス空間とは独立してセキュリティ解除鍵を格納するためのメモリ領域１２を有している。例えば、メモリ領域１２は、メモリセルアレイに対してローおよびローデコーダを追加して、拡張ローおよび拡張ローデコーダ１８ａを設けることにより実現することが可能である。

【００４０】

セキュリティ解除判定回路１４は、不揮発性レジスタ１３に格納されたセキュリティ登録錠とメモリセルアレイブロック１１内のメモリ領域１２に格納されたセキュリティ解除鍵の読み出し値を比較照合して比較照合して、セキュリティ解除の許可を行うか否かを判定する回路である。例えば、単純にセキュリティ登録錠とセキュリティ解除鍵が一致するかどうかを判定する一致回路を用いることが可能である。また、一方に対して何らかの演算を行った結果（ｘｏｒ演算のような単純なものであってもよいし、一方向ハッシュ変換のようなものであってもよい）と、他方とを比較する比較回路であってもよい。

【００４１】

判定結果保存レジスタ１５は、セキュリティ解除判定回路１４の出力結果（比較照合結果）を各メモリセルアレイブロック毎に保存するレジスタであり、揮発性のレジスタを用いることができる。

【００４２】

メモリセルアレイデータ出力切り替え回路１６は、セキュリティ解除判定回路１４からの出力信号が、セキュリティ解除鍵とセキュリティ登録錠の比較照合結果が一致したことを示している場合に、該当ブロックからの読み出しデータの外部出力を許可する回路である。例えば、出力マルチプレクサ等を用いることが可能である。

【００４３】

このように構成された本実施形態の不揮発性半導体記憶装置は、例えば以下のようにして動作する。メモリセルアレイからのデータ読み出しを行う際に、外部からアドレス１０５が入力されると、ブロック、カラム、ローに分解されて各々

ブロックデコーダ１０、カラムデコーダ１７、ローデコーダ１８でデコードされ、あるメモリセルアレイブロック１１のメモリセルが選択され、データが読み出される。メモリセルアレイブロック１１から読み出されたデータ１０３はメモリセルアレイデータ出力切り替え回路１６に入力され、メモリセルアレイデータ出力切り替え回路１６は、セキュリティ解除信号１０１が有効な場合にのみメモリセルアレイブロック１１からの読み出しデータ１０３をそのまま出力データ１０６として出力する。一方、セキュリティ解除信号１０１が無効な場合には、例えばメモリセルが全て消去状態である場合の値等、偽データを出力データ１０６として出力する。これにより、セキュリティ解除信号１０１が無効な場合には本実施形態の不揮発性半導体記憶装置を用いたシステムは正常動作しなくなる。

【００４４】

上記セキュリティ解除信号１０１は、セキュリティ解除判定回路１４からの出力（セキュリティ解除信号）１０２によって生成される。選択メモリセルが存在するメモリセルアレイブロック内のメモリ領域１２に格納されているセキュリティ解除鍵の読み出しデータ１０７と、不揮発性レジスタ１３に格納されているそのメモリセルアレイブロックに対応するセキュリティ登録錠の読み出しデータ１０８とが一致する場合、セキュリティ解除判定回路１４は両者が一致したことを示す信号を出力し、これによりセキュリティ解除信号１０１が有効になる。

【００４５】

セキュリティ解除判定回路１４からの出力１０２をそのままセキュリティ解除信号１０１としてメモリセルアレイデータ出力切り替え回路１６に入力してもよいが、本実施形態において、セキュリティ解除信号１０１の値をブロック毎に揮発性のレジスタ１５に保存しているのは、アクセス速度を向上させるためである。

【００４６】

外部からアドレス１０５が入力されると、ブロックデコーダ１０によりブロックアドレスがデコードされて対応するレジスタ１５が選択され、そのレジスタ１５が保持している値がセキュリティ解除信号１０１として出力される。この場合、メモリにアクセスする度にセキュリティ解除鍵１０７およびセキュリティ登録

錠１０８の読み出しやセキュリティ解除判定を行う必要が無くなるので、アクセス速度を低下させることなく読み出しデータの出力を制御することができる。

【００４７】

揮発性のレジスタ１５に、予めセキュリティ解除鍵とセキュリティ登録錠との比較照合結果（セキュリティ解除判定結果）を保持しておくために、例えば、装置起動時やリセット時にデバイス内部のパワーオンまたはリセット信号をトリガーとしてセキュリティ認証命令がデバイス内部で自動発行されるようにして、セキュリティ認証命令を意識する必要が無いように実装してもよい。またはセキュリティ認証命令をユーザが発行するコマンドとして用意してもよい。ここで、コマンドは、ユーザが発行する専用のコマンドであっても、他のコマンド（例えばアレイリードモード遷移コマンド）等によって同時に実行される形であってもよい。

【００４８】

このセキュリティ認証命令により、全てのブロックまたは一部のブロックに対して順にセキュリティ解除鍵１０７とセキュリティ登録錠１０８とを読み出してセキュリティ解除判定回路１４によって比較照合し、その結果を対応するブロックの揮発性レジスタ１５に書き込んでいく。これを全ブロックに対して順次行う。この動作を実行するための回路構成としては、専用のステートマシンにて実現してもよいが、プログラムやイレースアルゴリズムを実現するために内蔵されているステートマシンやマイクロプロセッサにて構成することも可能である。

【００４９】

この際、セキュリティが不要なブロックに対しては、レジスタ１５の一部を不揮発性レジスタで構成し、保持される値をセキュリティ解除が許可される値に固定しておいてもよい。これにより、セキュリティ解除が許可される値に固定されたブロックに対しては、セキュリティ解除鍵の値によらず、アクセスを行うことが可能になり、書き換え後にセキュリティ解除鍵を再設定する必要がなくなる。よって、ＢＩＯＳやファームウェア等のようにシステム動作時にはＲＯＭとして働き、書き換えが不要な用途では、この不揮発性半導体記憶装置を用いたシステムによれば、セキュリティの存在を意識する必要が無くなる。

【００５０】

このように予めセキュリティ解除判定を一括して行ってもよいが、各ブロック毎にセキュリティ解除判定を行ってもよい。例えば、各ブロックに初めにアクセスしたときにセキュリティ解除鍵とセキュリティ登録錠との比較照合を行ってその結果を揮発性レジスタ１５に登録しておき、２回目以降のアクセスで揮発性レジスタ１５に保持されている値を用いることができる。

【００５１】

不揮発性半導体記憶装置にシステムが組み込まれた状態で、正規ユーザがあるブロックを書き換える場合には、以下のようなフローにより動作が行われる。まず、最初に書き換え対象となるメモリセルアレイブロック１１を一括消去する。このとき、対象ブロック内のセキュリティ解除鍵１２も同時に消去される。次に、メインメモリブロック領域１１ａに更新データを書き込み、最後にメモリ領域１２に正規のセキュリティ解除鍵を、例えばセキュリティ解除鍵設定命令を発行することによって書き込む。なお、セキュリティ解除鍵設定命令を発行せずに、通常のデータ入力コマンドシーケンスにセキュリティ解除鍵データを含めることも可能である。

【００５２】

このように、正規のセキュリティ解除鍵の設定後に始めて、書き換えを行ったブロックへの正常なアクセスが可能になる。不正ユーザがプログラムやデータを不正に改ざんする場合、セキュリティ解除鍵が分からないために改ざんしたデータやプログラムを読み出すことができず、データやプログラムが改ざんされたシステムは正常に動作しなくなる。

【００５３】

このようなセキュリティ解除鍵設定命令を解釈する命令解釈回路や設定命令を実行する回路は、内蔵のステートマシンまたはマイクロプロセッサにて構成することが可能である。このような回路を内蔵させる場合、データのプログラムやイレースアルゴリズムを実現するためのステートマシンやマイクロプロセッサと一体化させてもよい。また、この命令により書き込まれる内容は、外部から入力された値をそのまま用いても良く、または、書き込まれているセキュリティ登録錠

またはセキュリティ解除鍵を何らかの不正手段で直接読み出されても、その値をコピーして直接書き込むことができないように、図２で示されるような一方向ハッシュ変換回路を通過させた値であってもよい。さらに、セキュリティ登録錠設定命令についても、セキュリティ解除鍵設定命令と同様の構成で実現することができる。

【００５４】

さらにセキュリティを高めるためには、セキュリティ解除鍵およびセキュリティ登録錠の値を容易に読み出されないように工夫することができる。例えば、図２に示すように、不揮発性レジスタ１３およびメモリ領域１２にセキュリティ登録錠およびセキュリティ解除鍵を書き込む際に、一方向ハッシュ変換回路２４等を用いて一方向ハッシュ関数等によりデータ２０２を変換した値２０４を書き込むようにする。これにより、セキュリティ解除鍵およびセキュリティ登録錠の変換値として、本発明の不揮発性半導体記憶装置に保持されているデータを読み出すことができたとしても、不正ユーザは変換前のセキュリティ解除鍵を知ることは困難であり、不正書き換えを行ったデータの読み出し許可を得ることも困難になる。このデータ２０２は、ブロックへの通常のデータ入出力と同様の経路（例えばデータバス）から入力することができる。

【００５５】

さらに、セキュリティ解除鍵およびセキュリティ登録錠の値を不揮発性半導体記憶装置の外部に読み出す手段を設けないことにより、セキュリティ登録錠およびセキュリティ解除鍵が不正ユーザに洩れるのを防ぐことができる。セキュリティ登録錠については、不揮発性レジスタ１３への書き込み手段だけを設けて読み出し手段を設けなければ良い。また、セキュリティ解除鍵はブロック内のメモリ領域に置かれているが、通常ユーザ（システム）が外部から指定するアドレス空間とは独立しているため、セキュリティ解除鍵を直接外部に読み出せないようにすることができる。例えば、（１）セキュリティ解除鍵１２のデータバス１０７を外部への出力可能なデータバス１０３に接続しない、（２）セキュリティ解除鍵１２へのアクセス中（拡張ローデコーダ選択状態中）は出力切り替え回路１６または他の部分（出力マルチプレクサや出力バッファ部等）により出力を禁止す

る等の制御を行うことが考えられる。

【００５６】

セキュリティ登録錠の書き換えを禁止することにより、不正ユーザによってセキュリティ登録錠自体が書き換えられるのを防ぐことができる。例えば、セキュリティ登録錠の不揮発性レジスタ内にロックフラグ格納領域（ｂｉｔ）を設けて、セキュリティ登録錠設定命令実行時にそのロックフラグを設定する。そして、ロックフラグが設定されているブロックには、セキュリティ登録錠設定命令が実行されないようにすればよい。このロックフラグは後で解除することもできるが、解除できないようにした方がセキュリティをより高めることができる。または、セキュリティ登録錠をワンタイムプログラマブルロム（ＯＴＰ－ＲＯＭ）を用いて設定してもよい。

【００５７】

さらに、セキュリティ解除鍵に対する繰り返し攻撃によってセキュリティが解除されるのを防ぐために、メモリ領域１２内にセキュリティ解除鍵の設定フラグを設けて、セキュリティ解除鍵の書き込み時に設定フラグを自動または手動で設定することにより、該当メモリセルアレイブロックへの追加書き込みを禁止することができる。

【００５８】

この場合、メモリセルアレイブロックへの追加書き込みができないため、セキュリティ登録錠の値を知らない不正ユーザがセキュリティを破るためには、まず、改ざんしたいメモリセルアレイブロックを消去する。次に、ブロックに改ざんデータを書き込んで、セキュリティ解除鍵を適当に設定し、セキュリティ解除鍵が正しいが否かを書き込んだデータを読み出せるか否かで判断する。そして、読み出せない場合には、異なるセキュリティ解除鍵に変えて同じ動作をセキュリティ解除が成功するまで試みる。しかし、このような繰り返し攻撃は、以下のような点から現実的ではない。まず、フラッシュメモリに代表される不揮発性半導体記憶装置には書き換え回数に制限があり、繰り返し攻撃自体が装置の劣化を招き、装置寿命を縮める行為となるからである。また、繰り返し攻撃はブロックの一括消去、ブロックへの書き込みおよびセキュリティ解除鍵設定を繰り返すことに

よって実行されるが、フラッシュメモリ等ではブロック消去およびブロックへのデータ書き込みに比較的時間がかかるからである。

【００５９】

さらに、セキュリティ解除鍵をメモリ領域１２に書き込み中に、自動的にウェイト動作を要求するような回路を設けることにより、さらに書き込み動作に時間がかかる。よって、不正ユーザによるセキュリティ解除鍵への繰り返し攻撃の際に、一回の攻撃に要する時間が長くなって、現実的な時間内にセキュリティ解除鍵を発見することが困難になる。例えば、セキュリティ解除鍵設定命令を実行する回路であるステートマシンまたはマイクロプロセッサの動作にウェイト回路またはウェイトルーチン（コード）を内蔵させることによって実現することができる。ステートマシンによるウェイト回路の例としては、内部クロックで動作するカウンタ回路を用意して、カウンタが規定値になるまでその状態で待つような構成を利用することができる。フラッシュメモリにおいては、このようなウェイトはプロファイルやイレース電圧をメモリセルにある時間印加するための回路またはマイクロプロセッサルーチンを利用することも可能である。

【００６０】

さらに、本発明によれば、不正な書き換えに対する制限を設けたブロックに書き換えを行う以外には、セキュリティ機能を有さない通常の不揮発性半導体記憶装置と同様に使用することが可能であるので、既存のシステムに組み込むことで、容易にセキュリティ機能を与えることが可能である。この場合、前提として、システムのバージョンアップや不具合修正時にはＲＯＭとして使用するＢＩＯＳやファームウェア用途を想定しており、このような用途での不正（一般）ユーザによる書き換えを防止することを目的としている。システム組み込み状態での書き換えを必要としないシステムでは、既存のシステムにそのまま組み込むことで容易にセキュリティ機能を与えることが可能である。なお、制限を設けたブロックに書き換えを行う場合には、システム側で対応しても良いが、内容書き換え時にシステムに接続される外部の書き換え器（ＲＯＭライタ）が対応するように構成してもよい。さらに、外部の書き換え器が不揮発性半導体記憶装置に対する書き換え命令プログラムルーチンを含むような構成の場合、既存のシステムにその

まま組み込むことで、容易にセキュリティ機能を与えることが可能である。

【００６１】

本発明は、例えばＢＩＯＳやファームウェア等、ソフトウェアを格納するために用いられるフラッシュメモリやフラッシュメモリを内蔵したＬＳＩ等に適用することが可能である。

【００６２】

このような用途では。ソフトウェアのバージョンアップや不具合修正のために、システム上で書き換え可能な手段を用意する場合が多い。これは、機器の小型化に伴ってソフトウェアが書き込まれた不揮発性半導体記憶装置自体を差し替えることが困難になってきたこと、および開発期間やソフトウェアの寿命が短くなってソフトウェアの書き換えに対する要求が高まっていること等が背景にある。この場合には、ユーザによる不正なソフトウェアの改ざんを防止したいという要求もある。

【００６３】

そこで、本発明の不揮発性半導体記憶装置によれば、不正改ざんに対する制限を設けたブロックに対するシステム上での書き換えをセキュリティ解除鍵を知らないユーザが行うと、改ざんされたブロックのソフトウェアコードやデータをシステムが読み出すことができなくなり、システム自体を使用することができなくなる。また、セキュリティ解除鍵を知っているユーザまたはシステム製造者は、データ書き換え後にセキュリティ解除鍵を設定し直すことにより、書き換えたブロックを有効に活用することができる。なお、本発明の不揮発性半導体記憶装置において、セキュリティ解除鍵やセキュリティ登録錠が設定されていない状態では、自由に読み書きすることも可能である。

【００６４】

【発明の効果】

以上詳述したように、本発明によれば、セキュリティ解除鍵を知っている正規ユーザによるシステム上でのソフトウェアやデータの書き換えは許可するが、不正な書き換えは防止する機能を提供することができる。

【００６５】

また、データ書き換えを行わない通常の使用状態では、外部システムとセキュリティ解除鍵のやり取りをしないために、本発明の不揮発性半導体記憶装置を組み込んだシステムにセキュリティ解除鍵を保持しておく必要はない。よって、本発明の不揮発性半導体記憶装置を組み込んだシステムからセキュリティ解除鍵を不正に知ることができず、安全なセキュリティ機能を提供することができる。

【００６６】

また、通常の使用状態では外部システムとセキュリティ解除鍵のやり取りをしないために、従来の不揮発性半導体記憶装置と互換性を有しながらセキュリティ機能を提供することができる。また、通常の使用状態では、組み込むシステム側において、本発明の不揮発性半導体記憶装置を利用するためのソフトウェアの対応は不要である。または、例えば認証動作がユーザ（システム）からの命令によって起動される構成の場合にはシステム側のソフトウェアでこの命令を発行するような対応が必要になるが、この場合にも簡単なものでよい。よって、ハードウェアの追加は不要である。

【００６７】

また、セキュリティ解除鍵を不正に知るために不正改ざん者により行われる繰り返し攻撃は現実的ではなく、強固なセキュリティ機能を提供することができる。

【００６８】

さらに、従来よりも小規模、かつ、簡単な回路で不正な書き換えを防止する機能を提供することができる。

【図面の簡単な説明】

【図１】

本発明の一実施形態である不揮発性半導体記憶装置の構成を説明するためのブロック図である。

【図２】

本発明の一実施形態である不揮発性半導体記憶装置において、一方向ハッシュ変換回路を設けた構成を説明するためのブロック図である。

【図３】

従来のデータ改ざん防止回路が内蔵された半導体メモリの構成を示すブロック図である。

【符号の説明】

１０　ブロックデコーダ

１１　一括消去可能メモリセルアレイブロック

１１ａ　メインメモリブロック領域

１２　セキュリティ解除鍵を格納するメモリ領域

１３　セキュリティ登録錠を格納する不揮発性レジスタ

１４　セキュリティ解除判定回路

１５　ブロックｎに対する判定結果保存レジスタ

１６　メモリセルアレイデコーダ切り替え回路

１７　カラムデコーダ

１８　ローデコーダ

１８ａ　拡張ローデコーダ

１８ｂ　メインメモリ用のローデコーダ

１９　アドレスプリデコーダ

２３　アドレスデコーダ

２４　一方向ハッシュ変換回路

３０　一方向ハッシュ変換されたキーコードを保持する内部レジスタ

３１　入力された暗号に対する復号回路（保全通信回路）

３２　一方向ハッシュ変換回路

３３　機能制限解除判定回路（比較回路）

３４　機能制限解除信号

１０１　セキュリティ解除信号（読み出しデータ出力許可信号）

１０２　セキュリティ解除信号

１０３　メモリセルアレイブロックからの読み出しデータ

１０４　ブロックアドレス信号

１０５、２０１　装置外部からのアドレス入力

１０６　装置外部へのデータ出力

１０７　セキュリティ解除鍵の読み出しデータ

１０８　セキュリティ登録錠の読み出しデータ

２０２　装置外部からのデータ入力

２０３　アドレス信号

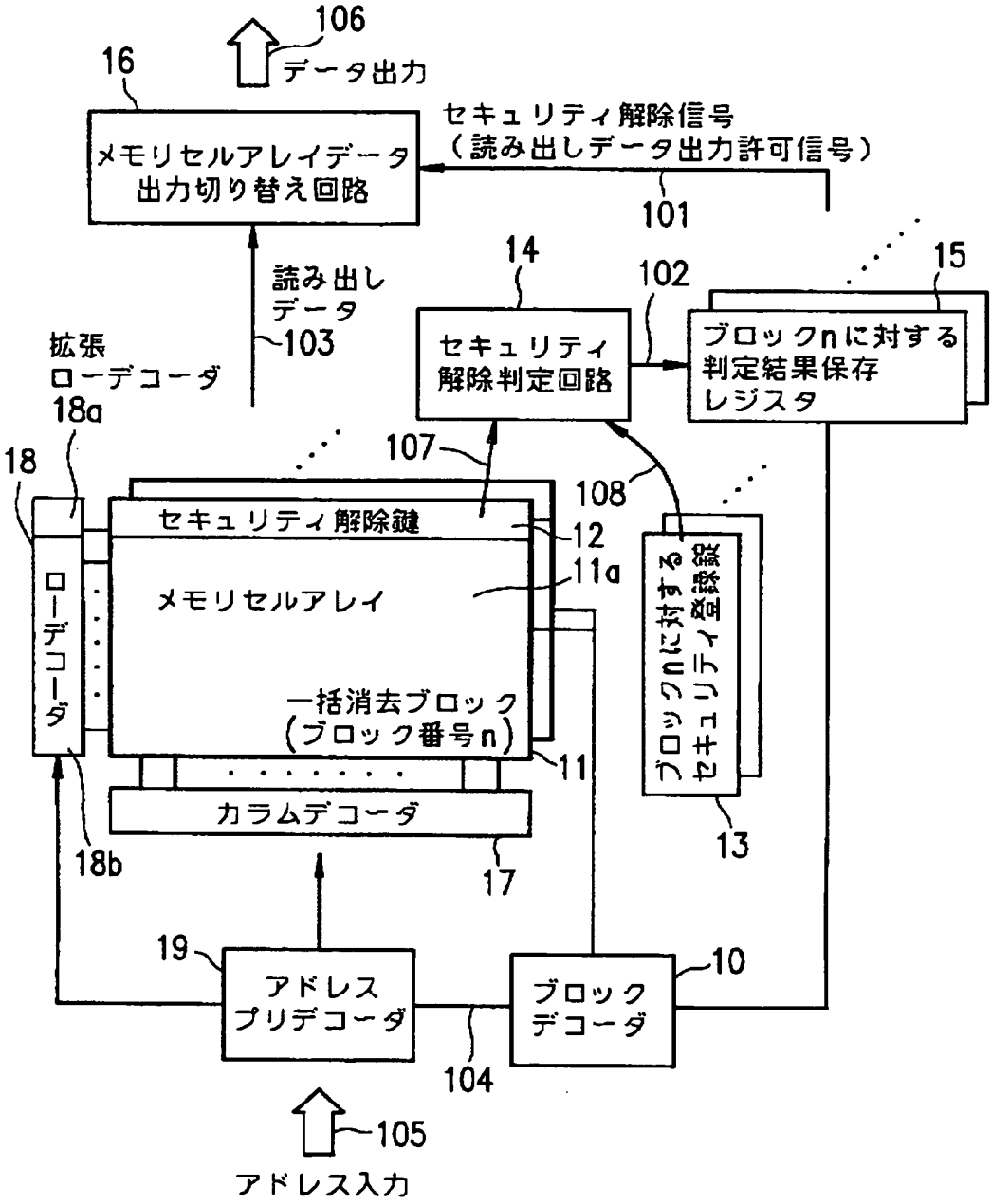
２０４　データを一方向ハッシュ変換回路により変換した値

Ｉｖ１　復号化されたキーコード

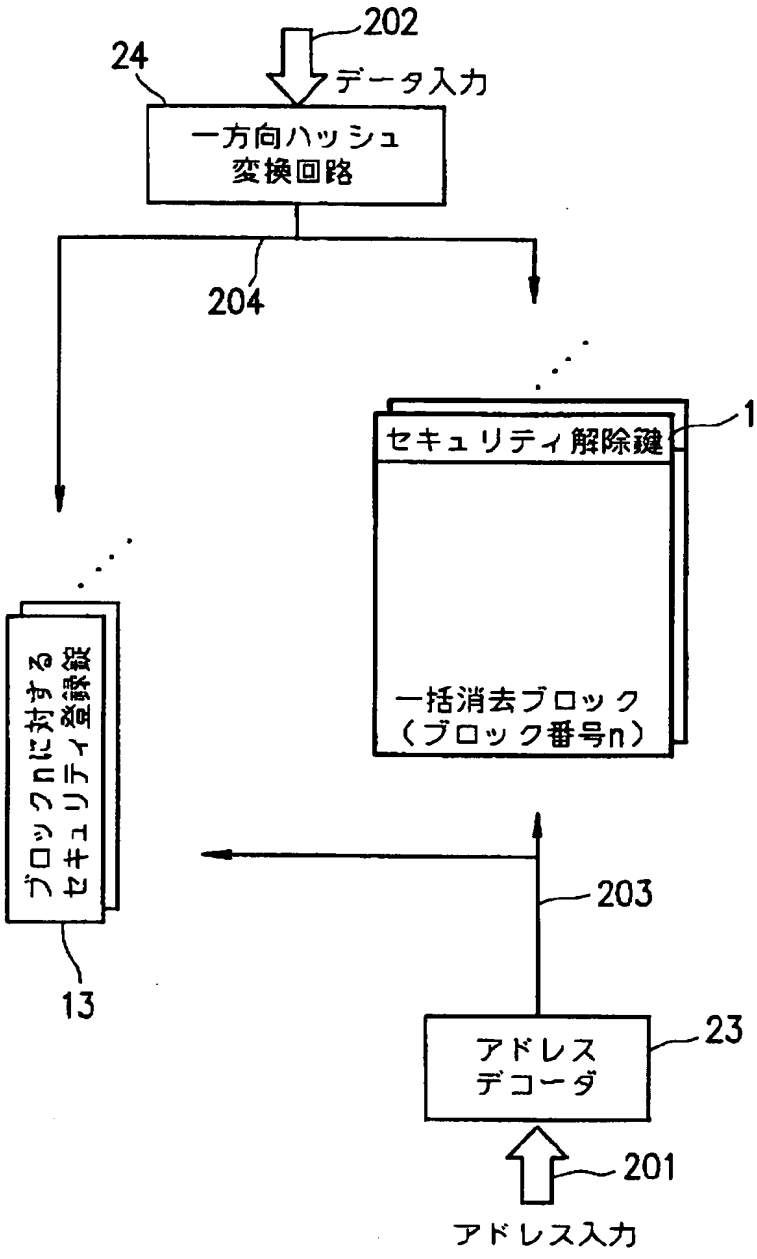
Ｉｖ２　一方向ハッシュ変換されたキーコード

【書類名】　図面

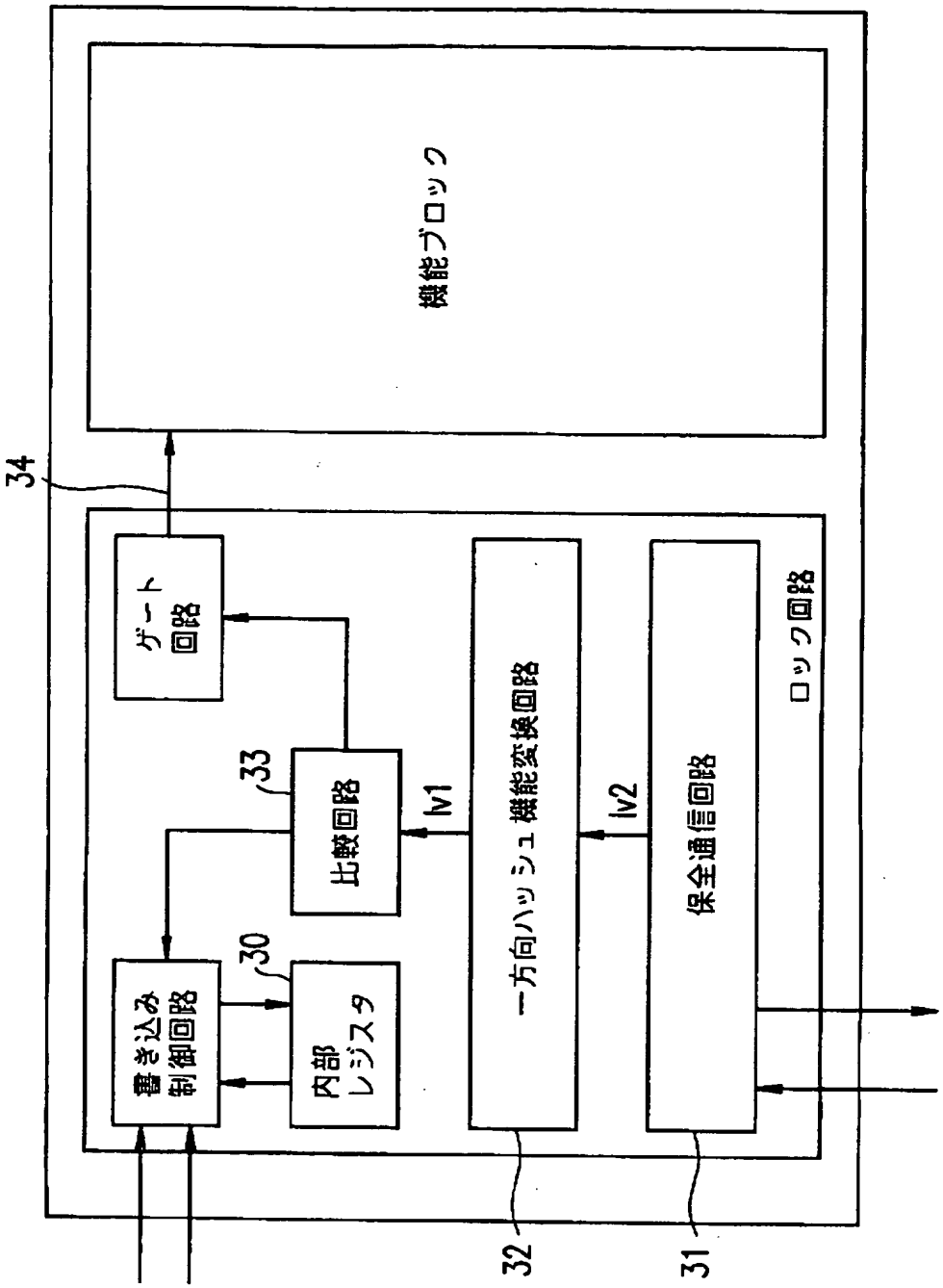
【図１】


106
データ出力
16
メモリセルアレイデータ
出力切り替え回路
セキュリティ解除信号
（読み出しデータ出力許可信号）
101
読み出し
データ
103
14
102
15
セキュリティ
解除判定回路
ブロックnに対する
判定結果保存
レジスタ
拡張
ローデコーダ
18a
18
107
108
セキュリティ解除鍵
12
11a
メモリセルアレイ
ローデコーダ
一括消去ブロック
（ブロック番号n）
11
ブロックnに対する
セキュリティ登録
13
カラムデコーダ
17
18b
19
アドレス
プリデコーダ
ブロック
デコーダ
10
104
105
アドレス入力

【図２】


202
データ入力
24
一方向ハッシュ
変換回路
204
セキュリティ解除鍵
12
一括消去ブロック
（ブロック番号n）
ブロックnに対する
セキュリティ登録鍵
13
203
アドレス
デコーダ
23
201
アドレス入力

【図３】


機能ブロック
34
ゲート回路
33
比較回路
lv1
一方向ハッシュ機能変換回路
lv2
保全通信回路
ロック回路
30
書き込み制御回路
内部レジスタ
32
31

【書類名】　要約書

【要約】

【課題】　データ改ざんを防ぎ、セキュリティ解除鍵が解読されにくく、不正ユーザによる認証に対する繰り返し攻撃に強い不揮発性半導体記憶装置を得る。

【解決手段】　ブロック１１内のメモリ領域１２にセキュリティ解除鍵が格納され、ブロック毎に対応するセキュリティ登録錠が不揮発性レジスタ１３に格納されている。両者をセキュリティ解除判定回路１４により比較照合し、一致した場合にデータ出力許可回路１６が正規データ出力を許可する。データ書き換え時にブロック消去によりメモリ領域１２のセキュリティ解除鍵も消去され、読み出し制限を解除するためには更新データを書き込み後、セキュリティ解除鍵を再びメモリ領域１２に書き込む。正しいセキュリティ解除鍵を知らない不正ユーザがデータを書き換えるとデータを読み出せず、システムが使用不可能になる。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５０４９〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　　大阪府大阪市阿倍野区長池町２２番２２号
氏　名　　シャープ株式会社